)ʃᵘ Cᴏᶜ

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Kobayashi et al.   Attorney Docket No.: GENSP151

Patent: 6,845,450 B1   09,652,415   Issued: January 18, 2005

Title: DISPLAY UNIT STORING AND USING A
CRYPTOGRAPHY KEY

REQUEST FOR CERTIFICATE OF CORRECTION
OF OFFICE MISTAKE
(35 U.S.C. §254, 37 CFR §1.322)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Attn: Certificate of Correction

Dear Sir:

Attached is Form PTO-1050 (Certificate of Correction) at least one copy of which is

suitable for printing. The errors together with the exact page and line number where they occur,

and shown correctly in the application filed, are as follows:

CLAIMS:

1.   In line 12 of claim 1 (column 7, line 34) change "key form" to --key from--. This

appears correctly in Amendment B, After Final as filed on July 19, 2004, on page 3, paragraph 4,

line 9, as claim 12.

2.   In line 6 of claim 9 (column 8, line 10) change "key generate" to --key and

generate--. This appears correctly in Amendment B, After Final as filed on July 19, 2004, on

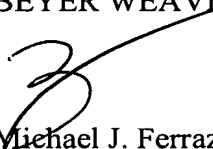page 4, paragraph 2, line 4, as claim 18.

3.   In line 19 of claim 16 (column 8, line 66) change "decrypted plural" to --decrypted plurality--. This appears correctly in Amendment B, After Final as filed on July 19, 2004, on page 6, paragraph 1, line 1, as claim 24.

4.   In line 12 of claim 17 (column 9, line 12) change "display is" to --display signal is--. This appears correctly in Amendment B, After Final as filed on July 19, 2004, on page 6, paragraph 3, line 9, as claim 26.

Patentee hereby requests expedited issuance of the Certificate of Correction because the error lies with the Office and because the error is clearly disclosed in the records of the Office. As required for expedited issuance, enclosed is documentation that unequivocally supports the patentee's assertion without needing reference to the patent file wrapper.

It is noted that the above-identified errors were printing errors that apparently occurred during the printing process. Accordingly, it is believed that no fees are due in connection with the filing of this Request for Certificate of Correction. However, if it is determined that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account 500388 (Order No. GENSP151).

<div style="margin-left:50%">

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

Michael J. Ferrazano
Registration No. 44,105

</div>

P.O. Box 70250
Oakland, CA 94612-0250
650-961-8300

9.   (previously presented) The display circuit as recited in claim 12, wherein when a source of

data is authenticated, said authenticating is performed using said unencrypted key based on data

sent and received on a path connected to said display unit.

10.   (previously presented) The display ciruit as recited in claim 9, wherein said path is

implemented using 1^2C protocol.

11.   (previously presented) The display circuit as recited in claim 12, further comprising a

master block external to said display unit that sends said unencrypted key-wherein when said

encrypted key is sent to said master block,-said master block stores said encrypted key in said non-

volatile memory.

12.   (previously presented) A display circuit for use in a display unit, said display circuit

comprising:

        a non-volatile memory storing a encrypted key, wherein said encrypted key is generated

from an unencrypted key according to an encryption protocol; and

        an integrated circuit coupled to said non-volatile memory, said integrated circuit receiving

said key in encrypted form and decrypting said key to generate a decrypted key, said integrated

circuit using said decrypted key wherein said integrated circuit comprises a key encryption

circuit receiving said unencrypted key, said key encryption circuit generating said encrypted key

from said unencrypted key according to said encryption protocol, a key decryption circuit

receiving said encrypted key and generating said decrypted key according to said encryption

protocol, a receiver adapted for receiving a plurality of digital data elements encoded in a display

signal, wherein said digital data elements represent a plurality of pixel data elements in an

encrypted form, said plurality of pixel data elements representing an image, and a data decryption

circuit receiving said plurality of digital data elements and generating said plurality of pixel data elements, wherein said image is generated on a display screen based on said plurality of pixel data elements, and wherein said display signal is received according to TMDS format.

13. - 17.   (Canceled)

18.   (previously presented) An integrated circuit, comprising:

a key encryption circuit adapted to receive an unencrypted key and generating an encrypted key from said unencrypted key according to an encryption protocol;

a key decryption circuit adapted to receive said encrypted key and generate said decrypted key according to said encryption protocol;

a receiver adapted to receive a plurality of digital data elements encoded in a display signal that is received according to TMDS format and that represents a plurality of pixel data elements in an encrypted form, wherein said plurality of pixel data elements represents an image that is generated on a display screen based on said plurality of pixel data element; and

a data decryption circuit adapted to receive said plurality of digital data elements and generate said plurality of pixel data elements.

19.   (previously presented) The integrated circuit as recited in claim 18 wherein the integrated circuit is

coupled to a non-volatile memory suitable for storing the encrypted key.

20.   (previously presented) The integrated circuit as recited in claim 19, further comprising:

a memory adapted to receive said encrypted key;

generating said image on a display screen based on said decrypted plurality of pixel data elements.

25.   (previously presented) The method as recited in claim 23, further comprising:

storing an encrypted key generated from an unencrypted key according to an encryption protocol in a non-volatile memory.

26.   (previously presented) Computer program product for using and storing a cryptography key, comprising:

computer code for receiving an unencrypted key

computer code for generating said encrypted key from said unencrypted key according to an encryption protocol

computer code for generating a decrypted key by decrypting the encrypted key according to said encryption protocol;

computer code for receiving a plurality of digital data elements encoded in a display signal wherein said display signal is received according to TMDS format, and wherein said digital data elements represent a plurality of pixel data elements in an encrypted form that represent an image;

computer code for decrypting said encrypted plurality of digital data elements;

computer code for generating said plurality of pixel data elements based upon said decrypted plurality of digital data elements;

computer code for generating said image on a display screen based on said decrypted plurality of pixel data elements; and

computer readable medium for storing the computer code.

(Also Form PT-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO.   : 6,845,450 B1

DATED   : January 18, 2005

INVENTOR(S) : Kobayashi et al.

It is certified that error appears in the above-identified patent and that said Letters Patent are hereby corrected as shown below:

In the Claims:

In line 12 of claim 1 (column 7, line 34) change "key form" to --key from--.

In line 6 of claim 9 (column 8, line 10) change "key generate" to --key and generate--.

In line 19 of claim 16 (column 8, line 66) change "decrypted plural" to --decrypted plurality--.

In line 12 of claim 17 (column 9, line 12) change "display is" to --display signal is--.

MAILING ADDRESS OF SENDER:

Michael J. Ferrazano
BEYER WEAVER & THOMAS, LLP
P.O. Box 70250
Oakland, CA 94612-0250

PATENT NO. 6,845,450 B1

No. of Additional Copies

→   1